MINISTÈRE
DES ARMÉES

Liberté
Égalité
Fraternité

Madame Florence Parly,

ministre des Armées

Montée en puissance du Commandement de la cyberdéfense

Rennes, le 7 septembre 2020

– Seul le prononcé fait foi –

Madame la préfète,
Mesdames et messieurs les officiers généraux,
Chers combattantes et cyber combattants, chers agents civils et militaires du ministère des Armées,
Mesdames et messieurs,

Je souhaiterais tout d'abord rendre hommage aux deux hussards parachutistes morts pour la France ce samedi. Deux soldats valeureux, qui ont tout donné pour la France et qui, jusqu'au bout, sont restés fidèles aux valeurs et au serment des hussards de Bercheny. Je m'incline devant leur mémoire et souhaite aujourd'hui que nous ne les oublions jamais.

Il y a un peu moins d'un an, nous étions déjà réunis ici, au quartier Stéphant, pour la naissance du commandement de la cyberdéfense, le ComCyber, dans la pierre bretonne. En effet, il y a un an, j'inaugurais le premier bâtiment entièrement dédié à la conduite des opérations cyber, baptisé Roger Baudoin en hommage à un pionnier français de la cryptographie.

Tout le monde ici sait que vous n'avez pas attendu d'avoir des murs à vous pour vous mettre en ordre de bataille. Mais l'inauguration du bâtiment Roger Baudoin a mis un coup d'accélérateur à votre montée en puissance. Et ce n'est pas étonnant : on ne peut pas attendre d'une armée qu'elle soit prête sans camp d'entraînement, ou opérationnelle sans centre de conduite des opérations. Disposer d'infrastructures sécurisées pour accueillir des activités sensibles, conçues pour être résilientes notamment dans le domaine énergétique, c'est absolument indispensable. C'est pourquoi nous investirons plus de 200 millions d'euros entre 2019 et 2025, dans la zone de la Maletière située à Saint-Jacques de la Lande, pour construire le temple de la cyberdéfense. Deux autres bâtiments seront ainsi construits d'ici 2025 pour accueillir les cybercombattants de demain.

Depuis un an, vous avez beaucoup grandi, forts de cette dynamique qui a permis de renforcer les synergies entre les différents acteurs de la cyberdéfense du ministère, notamment entre le commandement de la cyberdéfense, la direction générale de l'armement et la direction générale de la sécurité extérieure.

Vous vous êtes ancrés dans cette cyber-vallée européenne qui émerge à Rennes avec ces 70 entreprises spécialisées dans la cybersécurité et rassemblant plus de 2600 emplois. Vous avez tissé de nombreux partenariats industriels et académiques dans la région, conformément aux souhaits que j'avais formulés grâce notamment au Pôle d'excellence Cyber et avec le soutien des élus de la région. Vous êtes restés ouverts aux projets innovants, attentifs aux initiatives portées par des petites entreprises civiles ; et je suis donc très fière d'avoir rencontré aujourd'hui Glimps, Malizen et Sahar, les trois premières startups qui intègrent la Cyberdéfense factory, créée il y a tout juste un an.

Je suis ravie de constater également que la convention Brienne III signée il y a un an avec **la société d'investissement ACE Management, pour accélérer les financements de pépites françaises et européennes dans le domaine du cyber,** a porté ses fruits avec 5 investissements à son actif.

Vous avez aussi passé un cap dans l'organisation de vos capacités avec la création du groupement de la cyberdéfense des armées le 1er septembre 2020, il y a seulement 6 jours. Et je vous en félicite. Ce groupement permettra d'articuler les compétences de 3 unités différentes, implantées entre Rennes et Paris : le centre d'analyse de lutte informatique défensive, le centre des réserves de la préparation opérationnelle de cyberdéfense et enfin le centre d'audits de la sécurité des systèmes d'information. D'ici 2025, le groupement de la cyberdéfense des armées sera entièrement regroupé à Rennes et ses effectifs monteront progressivement en puissance pour atteindre 430 personnels contre 300 aujourd'hui.

Erigée en priorité nationale dans le Livre blanc de 2013, la cyberdéfense fait partie intégrante de la stratégie des armées. Sur les théâtres d'opérations comme sur le territoire national, nos forces sont directement exposées à la menace cyber. La lutte contre cette menace concerne tous les types d'action et tous les secteurs du cyberespace : la cyberprotection, la lutte informatique défensive, l'influence numérique, la lutte informatique offensive, ainsi que les moyens de commandement et d'entraînement. Afin de centraliser ces différentes missions au sein d'un commandement unique dédié, le COMCYBER a été créé en 2017.

Alors depuis trois ans, nous avons travaillé dur. Pour protéger les Français des menaces et des attaques ; pour les protéger, des conflits qui guettent, des capacités nouvelles qui se créent. Début 2019, nous présentions notre stratégie cyber, avec une petite révolution copernicienne et surtout un message adressé à nos adversaires : la France emploie et n'hésitera pas à employer l'arme cyber dans ses opérations militaires.

Pour accompagner la mise en œuvre de cette stratégie et nous doter des meilleures capacités opérationnelles, nous consacrons 1,6 milliard d'euros sur la période de la loi de programmation militaire 2019-2025. Nous investissons massivement pour acquérir les meilleurs moyens de cyberprotection et pour déployer des capacités de surveillance des systèmes les plus sensibles du ministère des Armées. Le reste des investissements concerne majoritairement les infrastructures, comme je vous le mentionnais plus tôt, ainsi que la préparation opérationnelle des 4 500 cybercombattants qui composeront notre cyberarmée d'ici 2025.

Aujourd'hui, c'est beaucoup de fierté que je ressens lorsque je vous vois porter le développement de notre cyberdéfense avec autant d'envie, de dynamisme et de professionnalisme. Et c'est très satisfaisant de voir nos différents projets se concrétiser peu à peu, et les succès se matérialiser les uns après les autres.

Car je pense que chacun a mesuré cette année à quel point les enjeux de cyberdéfense sont fondamentaux. Pouvions-nous imaginer il y a un an que nous passerions des mois entiers isolés les uns des autres, avec pour seul lieu et outil de travail, un ordinateur ? Nous avions certes anticipé la croissance du travail à distance, la nécessité de disposer d'infrastructures informatiques résilientes et de pouvoir communiquer les uns avec les autres via des réseaux connectés. Mais voir soudain la France connectée à distance, chaque jour à la même heure, avec internet comme seule fenêtre sur l'extérieur, je pense que personne ne peut se vanter de l'avoir vu venir.

Or, ce que nous savions depuis longtemps s'est concrétisée de la façon la plus visible. Aujourd'hui, nous faisons face à une pandémie. A une crise économique qui résulte de cette crise sanitaire. Il faut aussi que nous ayons conscience que la prochaine pandémie sera peut-être numérique.

Parler d'une pandémie numérique, cela donne à nouveau la sensation de plonger dans de la science-fiction. Mais c'est une menace plausible, que nous devons anticiper.

Je vous parle de menaces systémiques, je vous parle de cyber-attaques dangereuses, mais j'ai bien conscience que cela peut paraître parfois abstrait. Ce n'est pas évident de saisir les conséquences pratiques d'un cybercrime.

Alors je voudrais aujourd'hui vous faire part d'une attaque réelle qui a visé directement le ministère des Armées. **Nous sommes en juin 2019, au sein de l'hôpital d'instruction des armées Sainte-Anne, à Toulon.** C'est un hôpital de 400 lits qui est aujourd'hui le centre de référence dans le Var pour la prise en charge des traumatisés sévères, notamment des accidents de la route, des chutes ou blessures par armes. Il accueille naturellement des militaires évidemment, mais aussi de nombreux patients civils, comme ce fut le cas au plus fort de la crise sanitaire cette année.

Un jour de juin 2019, le réseau de l'hôpital militaire fait l'objet d'une attaque d'un Rançongiciel : comme le suggère son nom, un logiciel malveillant qui prend en otage des données personnelles et exige une somme d'argent pour débloquer les systèmes visés.

Deux ordinateurs et deux serveurs chiffrés de l'hôpital sont alors touchés et rendus inaccessibles. Si vous avez vu la dernière saison du Bureau des légendes, vous comprenez rapidement la course contre la montre qui s'engage pour éviter que le virus ne se propage et paralyse d'autres serveurs.

Les équipes informatiques de l'hôpital ont très bien réagi et ont réussi à stopper la propagation du logiciel. Un groupe d'intervention cyber du centre d'analyse de lutte informatique défensive (CALID) a été rapidement déployé pour récupérer les souches malveillantes du logiciel et effectuer des prélèvements sur les machines afin d'évaluer les conséquences de l'attaque.

Le bilan de cette cyberattaque, commise par un groupe de hackers individuels, est le suivant : 2 serveurs et 2 ordinateurs de l'hôpital militaire sont restés indisponibles pendant 3 semaines. Et les données des appareils contaminés n'ont pas pu être récupérées.

Alors on peut considérer que nous avons évité le pire. Imaginez si cette attaque n'avait pas été stoppée et s'était propagée sur l'ensemble des réseaux : impossible alors d'accéder aux données personnels des patients, impossible d'accéder à leur historique de soins, impossible de réaliser des scanners ou d'utiliser les équipements du bloc opératoire. Imaginez si cette attaque était arrivée au plus fort de la crise sanitaire : des respirateurs paralysés, des lits de réanimation en panne, l'impossibilité totale de prendre en charge les patients qui se présentent aux urgences.

Le cyber, c'est parfois un enjeu de vie ou de mort. Et cela touche chacun d'entre nous. C'est une guerre permanente, silencieuse et invisible, potentiellement dévastatrice lorsqu'elle se montre au grand jour.

Les attaques cyber, ça n'arrive pas seulement aux autres. Nous sommes tous concernés : les ministères, les institutions publiques, les banques, les entreprises, petites et grandes, les associations, parfois même les particuliers, nous pouvons tous être visés – et l'actualité de ces dernières heures l'illustre, qu'il s'agisse des attaques contre le tribunal de Paris ou le ministère de l'Intérieur.

Les failles existent partout et plus nous renforçons nos propres systèmes, plus les industriels et leurs sous-traitants deviennent une cible d'intérêt et une porte d'entrée vers nos réseaux. C'est pourquoi je crois dur comme fer, en la nécessité d'avoir une chaîne de cyberdéfense robuste « de bout en bout ». Nous ne devons pas laisser les réseaux des entreprises partenaires être le talon d'Achille de nos systèmes.

Avec cet objectif en ligne de mire, j'ai déjà signé une convention cyber avec les grands maîtres d'œuvre industriels pour garantir notre résilience collective.

Mais je souhaitais que nous allions plus loin. Je souhaitais que nous puissions apporter notre soutien aux petites et moyennes entreprises pour qui l'hygiène cyber a un coût.

J'ai donc le plaisir de vous annoncer la création de ce que nous avons appelé le « Diag Cyber », le diagnostic de cyberdéfense. Dans le cadre du plan Action PME, ce dispositif permettra aux startups et aux PME dont l'activité est liée à la défense d'évaluer la sécurité de leurs systèmes d'information, de déceler les failles éventuelles, et enfin d'être accompagnées dans la mise aux normes et le renforcement de la protection de leurs systèmes. Le ministère des Armées alloue 4,5

millions d’euros à ce dispositif et prendra en charge 50% des dépenses effectuées par les PME dans la limite de 14 000€ HT.

Le Diag Cyber, c’est un maillon de plus qui vient renforcer cette chaîne cyber de bout en bout. Il s’appuiera sur l’expertise de prestataires qualifiés par l’agence nationale de la sécurité des systèmes d’informations (ANSSI) ou référencés par le ministère des armées. C’est un dispositif de plus que vous mettrez en œuvre.

Alors n’oubliez pas une chose : vous êtes les champions du cyber. Et je sais que je peux compter sur vous. Que vous soyez chercheurs, ingénieurs, techniciens, cybercombattants, vous êtes tous unis par cette volonté d’exceller dans le cyber. Et ceci, pas pour la gloire, ni pour les honneurs. Simplement car vous avez conscience que construire notre cyberdéfense, c’est garantir notre souveraineté. Parce que vous savez que la résilience cyber, c’est la sécurité de notre société. Parce qu’enfin, vous savez que la France de demain, une France libre et belle où notre défense est assurée, c’est une cyber-puissance.

Vive la République ! Vive la France !